

Continuous Threat Monitoring Delivered by Menlo Security iSOC

Menlo Security iSOC complements the Menlo Security Isolation Core™ by closing security holes and eliminating security blind spots for SOC teams.

Benefits:

- Complements Menlo's isolate-or-block approach to stopping cyberattacks
- Closes security holes created by unintended policy gaps
- Provides proactive alerts for advanced threats such as phishing, malware, and BEC
- Increases the efficiency of SOC personnel

The Menlo Security Global Cloud Proxy with an Isolation Core™ provides malware-free web browsing without impacting the native user experience. It does this by routing all Internet traffic through a remote browser in the cloud, where it makes an isolate-or-block decision in real time. Known malicious content is blocked while all other content is isolated and a mirrored image is passed on to the endpoint. This Zero Trust approach effectively neuters all malicious intent without limiting large portions of the web.

But some policies may unintentionally create blind spots in your security posture—such as a policy that allows certain users to download an original document or access original content. In these instances, a targeted campaign could take advantage of these configurations.

Menlo Security iSOC

The Menlo iSOC service complements the Menlo Security Platform by acting as a sentinel, monitoring customers' Internet traffic and actions and alerting them of any threats to their organization.

More specifically, iSOC alerts on any threats caused by:

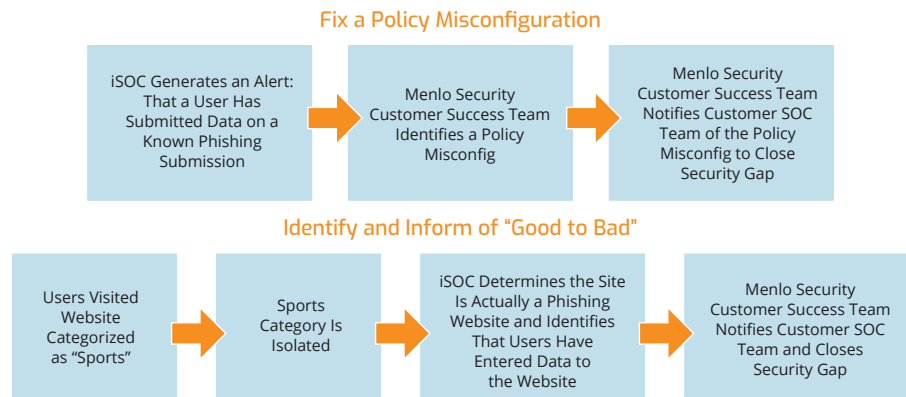
- Unintended policy gaps
- Malicious campaigns targeting an enterprise or individuals

iSOC provides prioritized and actionable threat intelligence that increases the efficiency of SOC personnel by reducing the number of alerts they have to process—thus helping to avoid alert fatigue. iSOC offsets the difficulty that many organizations have in finding, hiring, and retaining qualified threat hunters, incident response engineers, and security professionals. In addition, policy recommendations are made to fine-tune custom policies consistent with your vertical and similar customer profiles and based on Menlo Threat Research.



iSOC Example Use Cases:

iSOC provides prioritized and actionable threat intelligence to increase the efficiency of SOC teams.



Security without Compromise

The Menlo Security Global Cloud Proxy with an Isolation Core™ provides malware-free web browsing without impacting the native user experience. Large swaths of the Internet that may seem risky to security tools but are actually relevant to users' jobs can be opened, eliminating help desk requests while increasing productivity.

Organizations allow access to some websites without isolating them, which means that Menlo's Isolation Core™ cannot provide absolute protection when accessing the Internet. iSOC helps mitigate the risks associated with these types of policy gaps by monitoring the customer's Internet traffic as it flows through the Menlo platform to identify unintended policy gaps or misconfigurations and changes of risk classification from good to bad.

To find out how Menlo Security can provide your company with security without compromise against cyberattacks, visit menlosecurity.com or contact us at ask@menlosecurity.com.

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security has helped hundreds of Global 2000 companies and major government agencies achieve Secure Cloud Transformation. The company's Cloud Security Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. The company was named a Visionary in the Gartner Magic Quadrant for the Secure Web Gateway.
© 2020 Menlo Security, All Rights Reserved.

Contact us
menlosecurity.com
(650) 695-0695
ask@menlosecurity.com

